SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1 BUSINESS ETHICS, CONFLICT OF INTEREST AND COMPLIANCE (OCT 2014)

a. General: It is imperative that the Contractor and the services provided under this contract be free, to the greatest extent possible, of all Organizational and Personal Conflicts of Interest (OCI/PCI). Except as provided below, the Contracting Officer shall not maintain a contract with a Contractor that the Contracting Officer determines has, or has the potential for, an unresolved OCI/PCI. However, in accordance with FAR 9.503 Waiver, the Contracting Officer may contract with a Contractor that has an unresolved OCI/PCI if he/she determines that it is in the best interest of the Government to do so.

b. Definitions:

Actual OCI/PCI– means that the OCI/PCI is currently in existence as determined by the offeror's or Contractor's Compliance Officer and/or as determined by CMS. This form of OCI/PCI will require avoidance, neutralization or mitigation acceptable to CMS.

Affiliates – As defined in FAR 2.101 means associated business concerns or individual(s) if, directly or indirectly either one controls or can control the other; or a third party controls or can control both.

For purposes of this contract, affiliate control or influence may include, but is not limited to:

(a) Interlocking management or ownership (e.g., individuals serving in similar capacities in several companies);

(b) Identity of interests among family members such as spouse/domestic partner and/or any dependent of the respondent;

(c) Shared facilities and equipment;

(d) Common use of employees; or

(e) A business concern organized just prior to, or immediately following, the release of a solicitation or request for information, which has the same or similar management, ownership, or principal employees as the offeror or Contractor.

Any business, whether or not it is organized for profit or located in the United States or its outlying areas, or person may be found to be an affiliate. Control may be affirmative or negative and it is immaterial whether it is exercised so long as the power to control exists.

Apparent (Perceived) OCI/PCI – means that the OCI/PCI on first observation appears to be an actual or potential OCI/PCI, but may or may not be after analysis. Even if the apparent OCI/PCI is determined to be non-existent, in fact, this perception may still require further explanation.

Avoidance (Applicable to OCI only) – means Government action taken in one acquisition that is intended to prevent an OCI in that acquisition or in a future action. Methods of avoiding OCIs include, but are not limited to:

- Drafting the statement of work (SOW) to exclude tasks that require Contractors to utilize subjective judgment; or
- Obtaining advice from more than one source on any issue on which there are concerns about an OCI so that there is no area in which the Government is relying solely on the advice of any one of the sources; or

- Excluding an offeror from participation in a contract award.

Financial Interests/Relationships – means a healthcare related direct or indirect ownership or investment interest (including an option or non-vested interest) in any entity that exists through equity, debt, or other means and includes any indirect ownership or investment interest no matter how many levels removed from a direct interest.

A financial interest/relationship may arise from the following non-exclusive examples:

(a) Compensation, including wages, salaries, commissions, professional fees, or fees for business referrals;

(b) Current or known future contracts or arrangements includes, but is not limited to, an entity that may create one or more of the three forms of OCI;

(c) Consulting relationships, including commercial and professional consulting and service arrangements, scientific and technical advisory board memberships, or serving as an expert witness in litigation;

(d) Services provided in exchange for honorariums or travel expense reimbursements;

(e) Research funding or other forms of research support;

(f) Healthcare related investment in the form of stock or bond ownership, including healthcare sector investment only mutual funds;

(g) Healthcare business ownership or partnership interests;

(h) Patents, copyrights, and other intellectual property interests;

(i) Seeking or negotiating for prospective employment or business; or

(j) Gifts, including travel.

Mitigation (Applicable to both OCI & PCI) – means action taken by the Contractor to eliminate the OCI/PCI risk to an acceptable level on a present contract.

Neutralization (Applicable to OCI Only) – means excluding or restricting a Contractor from offering, as a prime or subcontractor, on future contracts while allowing the Contractor to perform on the instant contract. This method protects the government's interests in cases where the Contractor's work on the instant contract could be biased or impaired by virtue of its expectation of future work, or when the Contractor would have an unfair advantage in competing for award of the future work.

Organizational Conflict of Interest (OCI) – In accordance with FAR 2.101 Definitions, means that because of other activities or relationships with other persons, a person is unable, or potentially unable, to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is, or might be, otherwise impaired, or a person has an unfair competitive advantage.

For purposes of this contract, the OCI definition includes direct or indirect relationships including, but not limited to, the Contractor and its parent company, subsidiaries, affiliates, subcontractors, clients and principals.

Personal Conflicts of Interest (PCI) – A situation in which a person has a financial interest, personal activity, or relationship that could impair the person's ability to act impartially and in the best interest of the Government when performing under this contract.

(a) Among the sources of personal conflicts of interest are—

(i) Financial interests of the person, spouse/domestic partner and/or any other dependent of the person, as defined for Federal tax purposes;

(ii) Other employment or financial relationships (including seeking or negotiating for prospective employment or business) and,

(iii) Gifts, including travel.

(b) For example, financial interests referred to in paragraph (a)(i) of this definition may arise from—

(i) Compensation, including wages, salaries, commissions, professional fees, or fees for business referrals;

(ii) Consulting relationships;

(iii) Services provided in exchange for honoraria or travel expense reimbursements;

(iv) Research funding or other forms of research support;

(v) Healthcare related investments;

(vi) Real estate investments;

(vii) Patents, copyrights, and other intellectual property interests; or

(viii) Business ownership and investment interests.

Potential OCI/PCI – means that the OCI/PCI could become an actual OCI due to contingency events and/or as determined by CMS. This form of OCI/PCI will require avoidance, neutralization or mitigation acceptable to CMS.

Principal – As defined in FAR 52.203-13, Contractor Code of Business Ethics and Conduct, means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager, plant manager, head of a division or business segment, and similar positions).

Three (3) Types of OCIs/PCIs include:

Conflict Types	Definitions
Biased Ground Rules	Consists of situations in which a firm, as part of its performance of a Government contract, has helped (or is in a position to help) set the ground rules for another Government contract by, for example, writing the statement of work or the specifications, or establishing source-selection criteria. In these "biased ground rules" cases, the primary concern is that the firm could skew the competition, whether intentionally or not, in favor of itself and/or its affiliates.
Impaired Objectivity	Consists of situations where a firm's ability to render impartial advice to the government would be undermined by the firm's competing interests. The concern in impaired objectivity situations, including evaluation of services, is that a firm's ability to render impartial advice to the government will be undermined by the firm's relationship to the service being evaluated. These types of situations involve cases where a firm's work under one government contract could entail its evaluating itself, either through an assessment of performance under another contract or an evaluation of proposals.
Unequal Access to Information	"Unfair" access to non-public information – Consists of situations in which a firm has access to nonpublic information (including proprietary information and non-public source-selection information) as part of its performance of a Government contract and that information may provide the firm with a competitive advantage in a later competition for a Government contract. In these "unequal access to information" cases, the concern is limited to the risk of the firm gaining an unfair competitive advantage; there is no issue of bias.

c. Contractor Business Ethics, Conflict of Interest and Compliance Program Submissions: FAR 3.10 and FAR 52.203-13, Contractor Code of Business Ethics and Conduct, identify "…policies and procedures for establishment of Contractor codes of business ethics and conduct, and display of agency Office of Inspector General (OIG) hotline posters." The following chart is provided to clarify disclosure expectations under this contract:

FAR 52.203-13 Requirements Applicability (X = Applicable)	Contracts < $5 Million	Contracts ≥$5Million With a Small Business OR for Commercial Items (as Defined in FAR 2.101)	Contracts ≥$5Million With a Large Business (No Commercial Item Contracts)
OCI/PCI DISCLOSURES	X	X	X
PLAN FOR MONITORING/REPORTING OCIs/PCIs (Large Businesses Shall Incorporate OCI/PCI Monitoring/Reporting as Part of Its Compliance Program)	X	X	X
CODE OF CONDUCT	Not Required	X	X
COMPLIANCE PROGRAM	Not Required	Not Required	X

The following details are provided for respective disclosure expectations:

1. **Conflict of Interest Disclosures:** In accordance with FAR 3.10 and 52.203-13, Contractor Code of Business Ethics and Conduct, and this solicitation/contract, the Contractor shall have procedures in place to disclose all Organizational and Personal Conflicts of Interest (OCI/PCI) throughout the life of the contract. OCI/PCI disclosures shall be submitted as follows:

   (a) Initial Submission of OCI/PCI Information: The Contractor shall submit Conflict of Interest information identified in –

   - Attachment J.11, Business Ethics, Conflict of Interest and Compliance Submission by Offeror/Contractor (follow the format identified in the Attachment); and,

   - Attachment J.12, Personal Conflict of Interest (PCI) Financial Disclosure. Information shall be submitted with attachment J.12, information for each manager and key personnel who would be, or are involved with, the performance of this contract. If paragraphs H.1.e and H.1.f. of this clause are included, PCI Financial Disclosures are also required for all Board of Director members (if applicable) and principals of the organization as defined by FAR 52.203-13, Contractor Code of Business Ethics and Conduct. Provided at Attachment J.12, is a recommended PCI Financial Disclosure Template. The template is not required to be submitted; however, the information requested in the template shall be submitted.

(b) Conflict of Interest Disclosure During Contract Performance: The OCI/PCI Disclosure revisions shall be submitted to the Contracting Officer as follows:

i. Interim Revisions:

- At any time during the performance of this contract, if the Contractor learns of any actual, potential, or apparent OCI/PCI, whereby a reasonable business person might equate the OCI/PCI to one (1) of the three (3) types of OCIs/PCIs identified above, the Contractor shall notify the Contracting Officer in writing within five (5) business days of the identification of the actual, potential, or apparent OCI/PCI event. The Contractor shall then provide the changed information in Attachment J.11, Business Ethics, Conflict of Interest and Compliance Submission by Offeror/Contractor, and Attachment J.12, PCI Financial Disclosure Template, if necessary.

- Within 30 days of the Government or Contractor annual independent auditor review, if any findings require a change in the previous disclosures.

- When the Contracting Officer requests a revision.

- At least 45 days prior to a change due to proposed or planned business actions, e.g., acquiring or selling a business or business segment, changes in ownership of the organization holding the contract, etc.

ii. Annually:

1) **If Changes Are Required**:

1. Contracts with Options: 90 days prior to the exercise of an option for Contracting Officer consideration. If any period of performance is longer than 12 months, the annual certification shall be submitted no later than 30 days after each anniversary of the effective date of the contract. The Contractor shall provide the information in Attachment J.11, Business Ethics, Conflict of Interest and Compliance Submission by Offeror/Contractor, and Attachment J.12, PCI Financial Disclosure Template, if necessary. Submission of this information is not an indication of whether or not an option will be exercised.

2. Contracts without Options: The annual certification shall be submitted no later than 30 days after each anniversary of the effective date of the contract to the Contracting Officer. The Contractor shall provide the information in Attachment J.11, Business Ethics, Conflict of Interest and Compliance Submission by Offeror/Contractor, and Attachment J.12, PCI Financial Disclosure Template, if necessary.

2) If No Disclosure Changes Are Required: A written statement that "No OCI/PCI disclosure changes are required." shall be submitted to the Contracting Officer 30 days after the annual anniversary date or, if options, 90 days prior to option exercise.

3) If Annual Audit Is Required:

a) **When is Audit Required?:** An annual audit for the period January 1st through December 31st is required when paragraphs H.1.e. and H.1.f. of this clause are incorporated. The audit report will be submitted to the CMS Compliance Officer mailbox (ContractCompliance@cms.hhs.gov)

annually on March 31st of each year. If the Contractor has multiple CMS contracts, see H.1.f.3, Contractors with Multiple CMS Contracts Requiring Contractor Code of Business Ethics and Conduct Audits.

b) **Government Conducted Audit in Lieu of Contractor Independent Audit**: If the Government chooses to execute the annual audit in lieu of the contractor independent audit, the Contracting Officer will let the Contractor know by October 31st of the year being audited.

(c) Resolution: The Contracting Officer determines whether an OCI/PCI has been identified and whether the actual, potential or apparent OCI/PCI has been adequately mitigated. In cases whereby an OCI/PCI cannot be, or has not been, mitigated to the Contracting Officer's satisfaction, the Contracting Officer may take the following action including, but not limited to:

i. Request a waiver in accordance with FAR 9.503 Waiver, from the Head of the Contracting Activity; or

ii. Make changes to the scope of the contract; or

iii. Terminate the contract.

The Contractor's proposed OCI/PCI mitigation plan, if accepted, shall be incorporated into the contract.

2. Plan for Monitoring and Reporting OCI/PCI: The Contractor shall maintain effective oversight to verify compliance with conflict of interest safeguards including, but not limited to:

(a) Reviewing the information required by Attachment J.12, PCI Financial Disclosure Template, for each principal, officer and director of the organization, as well as managers and key personnel who would be, or are involved with, the performance of this contract. It is recommended that individuals who have not disclosed changes within the reporting period, submit an annual disclosure update to their Compliance Officer for review;

(b) Preventing conflicts of interest, prohibiting the use of non-public information accessed through this contract for personal gain, and obtaining a signed non-disclosure agreement to prohibit disclosure of non-public information accessed through this contract;

(c) Informing employees, through an employee education and training program, of their obligation to disclose and prevent conflicts of interest, not to use non-public information accessed through performance of this contract for personal gain, and to avoid even the appearance of personal conflicts of interest;

(d) Implementing internal polices and processes for:

(i) Conducting Internal and External Audits;
(ii) Policy Enforcement and Employee Disciplinary Actions;
(iii) Retention of Records;
(iv) Management of Subcontractors;
(v) Internal control systems; and,
(vi) Display of Fraud Hotline Poster(s) in accordance with FAR 52.203-14 Display of Hotline Poster(s).

(e) Reporting to the Contracting Officer any conflict of interest violations.

The Contractor shall attest/certify, with its Business Ethics, Conflict of Interest, and Compliance submission contained within its offer that it has or will put in place an OCI/PCI compliance program that meets the above criteria.

3. **Code of Business Ethics and Conduct (Code of Conduct):** In accordance with FAR 3.10 and 52.203-13, Contractor Code of Business Ethics and Conduct, the Contractor shall have a written Code of Conduct, if the contract value is greater than $5 Million. FAR 52.203-13 (b) and (c) identifies the requirements for the written Code of Conduct. If required, the Contractor shall submit the "Final" Code of Conduct to the Contracting Officer within 30 days of contract award, in accordance with FAR 52.203-13. Code of Conduct revisions shall be submitted in accordance with H.1.c.1(b) above.

4. **Business Ethics Awareness, Compliance Program and Internal Control System (Compliance Program):** In accordance with FAR 52.203-13, a Compliance Program is required if the contract value is over $5 Million, the Contractor has represented itself as a large business, and the contract is not for acquisition of commercial items. FAR 52.203-13(c) identifies the requirements for the Contractor's Compliance Program. The Contractor shall submit the "Final" Compliance Program to the Contracting Officer within 90 days of contract award, in accordance with FAR 52.203-13(c). Compliance Program revisions shall be submitted in accordance with H.1.c.1(b) above.

d. **Subcontractor Flow-Down Clause:** The prime Contractor is responsible for avoiding, neutralizing and mitigating all actual, potential, or apparent OCIs/PCIs of its Subcontractors, in accordance with this clause. Therefore, the prime Contractor shall flow-down H.1 Business Ethics, Conflict of Interest and Compliance, of this contract in all subcontracts. For Subcontractors, wherever the term "Contractor" is used, insert "Subcontractor."

H.2 RESTRICTIONS AGAINST DISCLOSURE

(a) The Contractor agrees to keep all information it gathers or analyzes or information the Government in the course of this contract/task order/delivery order furnishes in the strictest confidence. The Contractor also agrees that Government-provided information marked "For Official Use Only," "Confidential", or "Proprietary" must also be similarly protected and shall take all reasonable measures necessary to prohibit access to such information by any such person other than those Contractor employees needing such information to perform the work, i.e., on a need-to-know basis.

(b) The Contractor shall immediately notify the Contracting Officer in writing in the event it has been determined or the Contractor has reason to suspect a breach of this requirement.

(c) The Contractor shall require that all employees and consultants who are given access to such information sign a confidentiality and nondisclosure statement agreeing to safeguard the confidentiality of all such information gathered or provided to them hereunder as an integral condition of their employment.

(d) Upon the Government's written request, the Contractor shall provide the Contracting Officer with plans and procedures to ensure the confidentiality and physical security of information gathered or provided hereunder.

(e) The Contractor may "gather and analyze" information that is not furnished or owned by the Government. Such information shall not be subject to the restrictions in this clause.

H.3 CONTRACTOR TERMINATION CMS BUILDING PASS

In the event that the contractor terminates an employee working on this contract, or an employee working on this contract voluntarily leaves the employment of the contractor and that employee has been issued a contractor's badge by CMS for access to CMS Buildings; The contractor shall immediately take the following actions:

- Secure the CMS contractor's badge from the employee;

- Formally advise the contracting officer that the individual is no longer an employee of the contractor, and;

- Return the badge with the notification to the contracting officer.

H.4 SECURITY CLAUSE-BACKGROUND-INVESTIGATIONS FOR CONTRACTOR PERSONNEL

A. If applicable, Contractor personnel performing services for CMS under this contract, task order or delivery order shall be required to undergo a background investigation. CMS will pay for the background investigations.

B. After contract award, the CMS COR and the Emergency Management & Response Group (EMRG), with the assistance of the Contractor, shall perform a position-sensitivity analysis based on the duties contractor personnel shall perform on the contract, task order or delivery order. The results of the position-sensitivity analysis will determine first, whether the provisions of this clause are applicable to the contract and second, if applicable, determine each position's sensitivity level (i.e., high risk, moderate risk or low risk) and dictate the appropriate level of background investigation to be processed. Investigative packages may contain the following forms:

1. SF-85, Questionnaire for Non-Sensitive Positions, 09/1995
2. SF-85P, Questionnaire for Public Trust Positions, 09/1995
3. OF-612, Optional Application for Federal Employment, 12/2002
4. OF-306, Declaration for Federal Employment, 01/2001
5. Credit Report Release Form
6. FD-258, Fingerprint Card, 5/99, and
7. CMS-730A, Request for Physical Access to CMS Facilities (NON-CMS ONLY), 11/2003.

C. The Contractor personnel shall be required to undergo a background investigation commensurate with one of these position-sensitivity levels:

(i) High Risk (Level 6)

Public Trust positions that would have a potential for exceptionally serious impact on the integrity and efficiency of the service. This would include computer security of a major automated information system (AIS). This includes positions in which the incumbent's actions or inaction could diminish public confidence in the integrity, efficiency, or effectiveness of assigned government activities, whether or not actual damage occurs, particularly if duties are especially critical to the agency or program mission with a broad scope of responsibility and authority.

Major responsibilities that would require this level include:

a. development and administration of CMS computer security programs, including direction and control of risk analysis and/or threat assessment;
b. significant involvement in mission-critical systems;

c. preparation or approval of data for input into a system which does not necessarily involve personal access to the system but with relatively high risk of causing grave damage or realizing significant personal gain;
d. other responsibilities that involve relatively high risk of causing damage or realizing personal gain;
e. policy implementation;
f. higher level management duties/assignments or major program responsibility; or
g. independent spokespersons or non-management position with authority for independent action.

Approximate cost of each investigation: $3,500

(ii) Moderate Risk (Level 5)

Public Trust positions that have potential for moderate to serious impact on the integrity and efficiency of the service, including computer security. These positions involve duties of considerable importance to the CMS mission with significant program responsibilities that could cause damage to large portions of AIS. Duties involved are considerably important to the agency or program mission with significant program responsibility, or delivery of service. Responsibilities that would require this level include:

a. the direction, planning, design, operation, or maintenance of a computer system and whose work is technically reviewed by a higher authority at the High Risk level to ensure the integrity of the system;
b. systems design, operation, testing, maintenance, and/or monitoring that are carried out under the technical review of a higher authority at the High Risk level;
c. access to and/or processing of information requiring protection under the Privacy Act of 1974;
d. assists in policy development and implementation;
e. mid-level management duties/assignments;
f. any position with responsibility for independent or semi-independent action; or
g. delivery of service positions that demand public confidence or trust.

Approximate cost range of each investigation: $150 - $2,600

(iii) Low Risk (Level 1)

Positions having the potential for limited interaction with the agency or program mission, so the potential for impact on the integrity and efficiency of the service is small. This includes computer security impact on AIS.

Approximate cost of each investigation: $100

D. The Contractor shall submit the investigative package(s) to the EMRG within three (3) days after being advised by the EMRG of the need to submit packages. Investigative packages shall be submitted to the following address:

Centers for Medicare & Medicaid Services
Office of Operations Management
Emergency Management & Response Group
Mail Stop SL-13-15
7500 Security Boulevard
Baltimore, Maryland 21244-1850

E. The Contractor shall submit a copy of the transmittal letter to the Contracting Officer (CO).

F. Contractor personnel shall submit a CMS-730A (Request for Badge) to the EMRG. The Contractor and the COR shall obtain all necessary signatures on the CMS-730A prior to any Contractor employee arriving for fingerprinting and badge processing.

G. The Contractor must appoint a Security Investigation Liaison as a point of contact to resolve any issues of inaccurate or incomplete form(s). Where personal information is involved, EMRG may need to contact the contractor employee directly. The Security Investigation Liaison may be required to facilitate such contact.

H. After EMRG fingerprints contractor personnel and issues them a temporary CMS identification badge, the EMRG will send their completed investigative package to the Office of Personnel Management (OPM). OPM will conduct the background investigation. Badges will be provided by EMRG while contractor personnel investigative forms are being processed. The Contractor remains fully responsible for ensuring contract, task order or delivery order performance pending completion of background investigations of contractor personnel.

I. EMRG shall provide written notification to the CO with a copy to the COR of all suitability decisions. The shall then notify the Contractor in writing of the approval of the Contractor's employee(s), at that time the Contractor's employee(s) will receive a permanent identification badge. Contractor personnel who the EMRG determines to be ineligible may be required to cease working on the contract immediately.

J. The Contractor shall report immediately in writing to EMRG with copies to the CO and the COR, any adverse information regarding any of its employees that may impact their ability to perform under this contract, task order or delivery order. Reports should be based on reliable and substantiated information, not on rumor or innuendo. The report shall include the contractor employee's name and social security number, along with the adverse information being reported.

K. Contractor personnel shall be provided an opportunity to explain or refute unfavorable information found in an investigation to EMRG before an adverse adjudication is made. Contractor personnel may request, in writing, a copy of their own investigative results by contacting:

Office of Personnel Management
Freedom of Information
Federal Investigations Processing Center
PO Box 618
Boyers, PA 16018-0618.

L. At the Agency's discretion, if an investigated contractor employee leaves the employment of the contractor, or otherwise is no longer associated with the contract, task order, or delivery order within one (1) year from the date the background investigation was completed, then the Contractor may be required to reimburse CMS for the full cost of the investigation. Depending upon the type of background investigation conducted, the cost could be approximately $100 to $3,500. The amount to be paid by the Contractor shall be due and payable when the CO submits a written letter notifying the Contractor as to the cost of the investigation. The Contractor shall pay the amount due within thirty (30) days of the date of the CO's letter by check made payable to the "United States Treasury." The Contractor shall provide a copy of the CO's letter as an attachment to the check and submit both to the Office of Financial Management at the following address:

Centers for Medicare & Medicaid Services
PO Box 7520

Baltimore, Maryland 21207

M. The Contractor must immediately provide written notification to EMRG (with copies to the CO and the COR) of all terminations or resignations of Contractor personnel working on this contract, task order or delivery order. The Contractor must also notify EMRG (with copies to the CO and the COR) when a Contractor's employee is no longer working on this contract, task order or delivery order.

N. At the conclusion of the contract, task order or delivery order and at the time when a contractor employee is no longer working on the contract, task order or delivery order due to termination or resignation, all CMS-issued parking permits, identification badges, access cards, and/or keys must be promptly returned to EMRG. Contractor personnel who do not return their government-issued parking permits, identification badges, access cards, and/or keys within 48 hours of the last day of authorized access shall be permanently barred from the CMS complex and subject to fines and penalties authorized by applicable federal and State laws.

H.5 WORK PERFORMED OUTSIDE THE CONTINENTAL UNITED STATES AND ITS TERRITORIES (OCONUS)

The contractor, and its subcontractors, shall not perform any activities under this contract at a location OCONUS (outside the continental United States), including the transmission of data or other information OCONUS, without the prior written approval of the Contracting Officer. The factors that the Contracting Officer will consider in making a decision to authorize the performance of work OCONUS include, but are not limited to the following:

- All contract terms regarding system security;
- All contract terms regarding the confidentiality and privacy requirements for information and data protection;
- All contract terms that are otherwise relevant, including the provisions of the Statement of Objectives and what is defined in the technical requirements of a particular task order;
- All laws and regulations applicable to the performance of work OCONUS;
- Concurrence from the CMS SEMG Director or designee; and,
- The best interest of the Government.

In requesting the Contracting Officer's authorization to perform work OCONUS, the contractor must demonstrate that the performance of the work satisfies all of the above factors. If, in the Contracting Officer's judgment, the above factors are not fully satisfied, the performance of work OCONUS will not be authorized.

H.6 ADP SYSTEMS SECURITY REQUIREMENTS

In the performance of this contract, the Contractor agrees to comply with the ADP systems security requirements of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources", and with the ADP systems security policy of DHHS as outlined in Part 6 of the HHS ADP Systems Manual and in CMS's AIS Guide. The Contractor shall include this requirement in any subcontract awarded under this prime contract

H.7 HHSAR 352.224-70 PRIVACY ACT (JAN 2006)

This contract requires the Contractor to perform one or more of the following:
(a) design; (b) develop; or (c) operate a federal agency system of records to accomplish an agency function in accordance with the Privacy Act of 1974 (Act) [**5 U.S.C. 552a(m)(1)**] and applicable agency regulations. The term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Violations of the Act by the Contractor and/or its employees may result in the imposition of criminal penalties [**5 U.S.C. 552a(i)**]. The Contractor shall ensure that each of its employees knows the prescribed rules of conduct and that each employee is aware that he/she is subject to criminal penalties for violation of the Act to the same extent as Department of Health and Human Services employees. These provisions also apply to all subcontracts the Contractor awards under this contract which require the design, development or operation of the designated system(s) of records [**5 U.S.C. 552a(m)(1)**]. The contract work statement: (a) identifies the system(s) of records and the design, development, or operation work the Contractor is to perform; and (b) specifies the disposition to be made of such records upon completion of contract performance.

H.8 HIPPA BUSINESS ASSOCIATE CLAUSE (OCT 2013)

All Protected Health Information (PHI), as defined in 45 C.F.R. §160.103, that is relevant to this Contract, shall be administered in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA," 42 U.S.C. § 1320d), as amended, as well as the corresponding implementing regulations and this HIPAA Business Associate Clause.

a. Definitions:

All terms used herein and not otherwise defined, shall have the same meaning as in HIPAA, as amended, and the corresponding implementing regulations. Non-HIPAA related provisions governing the Contractor's duties and obligations, such as those under the Privacy Act and any applicable data use agreements, are generally covered elsewhere in the Contract.

The following definitions apply to this Contract Clause:

"**Business Associate**" shall mean the Contractor (and/or the Contractor's subcontractors or agents) if/when it uses individually identifiable health information on behalf of CMS, i.e. PHI, to carry out CMS' HIPAA-covered functions.

"**Covered Entity**" shall mean the portions of CMS that are subject to the HIPAA Privacy Rule.

"**Secretary**" shall mean the Secretary of the Department of Health & Human Services or the Secretary's designee.

b. Obligations and Activities of Business Associate:

Except as otherwise provided in this Contract, Business Associate, as defined above, shall only use or disclose PHI on behalf of, or to provide services to, Covered Entity in accordance with this Contract and the HIPAA Privacy and Security Rules.

Business Associate shall document in writing the policies and procedures that will be used to meet HIPAA requirements. The policies and procedures shall include the following, at a minimum:

1. Business Associate shall <u>not</u>:

    a. Use or disclose PHI that is created, received, maintained or transmitted by Business

Associate from, or on behalf of, Covered Entity other than as permitted or required by this Contract or as required by law;

b. Sell PHI; or,

c. Threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual for:

i. Filing a complaint under 45 CFR § 160.306;

ii. Testifying, assisting or participating in an investigation, compliance review, proceeding or hearing under 45 CFR Part 160; or

iii. Opposing any act or practice that is unlawful under HIPAA, provided there is a good faith belief that the practice is unlawful, the manner of opposition is reasonable, and the opposition does not involve the disclosure of PHI in violation of subpart E of Part 164.

2. Business Associate shall:

a. Have a security official who will be responsible for development and implementation of its security policies and procedures, including workforce security measures, to ensure proper security awareness and training (including security incident response and reporting), and security incident procedures, in accordance with this Contract, including this HIPAA Business Associate Clause and the Contract's clause entitled "CMS Information Security."

b. Use administrative, physical and technical safeguards to prevent use or disclosure of PHI created, received, maintained or transmitted by Business Associate from, or on behalf of Covered Entity only as provided for by this Contract. In doing so, it shall implement policies and procedures to address the following and, where applicable, ensure that such policies and procedures are also in conformance with this Contract's clause entitled "CMS Information Security:"

i. Prevent, detect, contain and correct security violations through the use of:
    1. Risk analyses (including periodic technical and nontechnical evaluations);
    2. Appropriate risk management strategies, including system activity review;
    3. Information access procedures for approving individual's access rights to PHI (including the implementation of workforce security measures to ensure continued appropriate role-based access to PHI), and technical policies and procedures to ensure compliance with grants of access (including unique user identification and tracking of users) and;
    4. The imposition of sanctions for violations.

ii. Limit physical access to its electronic information systems and the facility or facilities in which they are housed.

iii. Implement policies, procedures and physical security measures that will limit access to PHI through workstations and other devices, including access through mobile devices.

iv. Implement media controls covering the movement of devices containing PHI within or outside of the Business Associate's facility as well as the disposal and reuse of media containing PHI.

v. Implement appropriate administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability (including the use of contingency plans) of any electronic protected health information ("EPHI") it creates, receives, maintains or transmits from, or on behalf of the Covered Entity to prevent impermissible use, disclosure, maintenance or transmission of such EPHI. In the establishment of such safeguards, Business Associate shall consider its size, complexity and capabilities, as well as its technical infrastructure, and its hardware and software security capabilities.

c. Assess, and implement, where appropriate, any addressable implementation specifications associated with applicable PHI security standards.

d. Mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Contract.

e. Comply with the following Incident Reporting:

(a) Report to Covered Entity any security incident/breach involving unsecured PHI, of which it becomes aware, including those of its agents and subcontractors. The Business Associate shall report any violation of the terms of this contract involving PHI and any security incidents/breaches involving unsecured PHI to CMS within one (1) hour of discovery in accordance with the CMS Risk Management Handbook (RMH), specifically "RMH Vol II Procedure 7-2 Incident Handling Procedure" and "RMH Vol III Standard 7-1 Incident Handling." These procedures can be found at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html In addition, the Business Associate will also notify the CMS Contracting Officer and the Contracting Officer's Representative (COR) by email within one (1) hour of identifying such violation or incident.

(b) Upon Covered Entity's knowledge of any material security incident/breach by Business Associate, Covered Entity will provide an opportunity for Business Associate to cure the breach or end the violation consistent with the termination clause of this Contract. *See also* paragraph D. Term of Clause below.

f. Ensure that any agent or subcontractor agrees through a written contract, or other legally enforceable arrangement, to the same restrictions and conditions that apply through this HIPAA Contract Clause, when creating, receiving, maintaining or transmitting PHI from, or on behalf of, Covered Entity.

g. Upon Covered Entity's request:

i. Provide the Covered Entity or its designee with access to the PHI created, received, maintained or transmitted by Business Associate from or on behalf of the Covered Entity in the course of contract performance in order to ensure Covered Entity's ability to meet the requirements under 45 CFR § 164.524.

ii. Amend PHI as Covered Entity directs or agrees to pursuant to 45 CFR § 164.526.

h. Make its facilities and any books, records, accounts, and any sources of PHI, including any policies and procedures, that are pertinent to ascertaining its own compliance with this contract or the Covered Entity's compliance with the applicable HIPAA requirements, available to Covered Entity, or, in the context of an investigation or

compliance review, to the Secretary for purposes of the Secretary determining Covered Entity's compliance with the various rules implementing the HIPAA.

i. Document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

j. Provide to Covered Entity, or an individual identified by the Covered Entity, information collected under this Contract, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

k. Make reasonable efforts to limit the PHI it uses, discloses or requests to the minimum necessary to accomplish the intended purpose of the permitted use, disclosure or request.

c. Obligations of Covered Entity

Covered Entity shall notify Business Associate of any:

1. Limitation(s) in its Notice of Privacy Practices in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI;

2. Changes in, or revocation of, permission by an Individual to use or disclose their PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI; and,

3. Restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

d. Term of Clause

1. The term of this Clause shall be effective as of date of Contract award, and shall terminate when all of the PHI provided to Business Associate by the Covered Entity or a Business Associate of the Covered Entity, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity in accordance with “CMS Information Security” procedures. Business Associate shall not retain any PHI.

2. Security Incident/Breach:

Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall take action consistent with the terms of this Contract, and, as appropriate, the following:

i. Federal Acquisition Regulation (FAR) Contracts – Covered Entity may:

A. Terminate this Contract in accordance with FAR Part 49, Termination of Contracts, if the Business Associate does not cure the security incident/breach within the time specified by Covered Entity and/or cure is not possible; or,

B. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

ii. Other Agreements –Covered Entity shall either:

A. Provide an opportunity for Business Associate to cure the breach or end the violation

consistent with the termination terms of this Contract. Covered Entity may terminate this Contract for default if the Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; or,

B. Consistent with the terms of this Contract, terminate this Contract for default if Business Associate has breached a material term of this Contract and cure is not possible; or,

C. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

3. Returning or Destroying PHI:

Business Associate, as defined above, which includes subcontractors or agents of the Contractor, shall:

i. Upon expiration or termination of this Contract, for any reason, return or destroy all PHI received from Covered Entity or another Business Associate of the Covered Entity, as well as any PHI created, received, maintained or transmitted from or on behalf of Covered Entity, or another Business Associate of the Covered Entity, in accordance with this contract, including the “CMS Information Security” clause.

ii. In the event that Business Associate determines that returning or destroying the PHI is infeasible, provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon such notice that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Contract to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

e. Miscellaneous

1. A reference in this Contract to a section in the Rules issued under HIPAA means the section as in effect or as amended.

2. The respective rights and obligations of Business Associate under paragraph D.3.b of the section entitled "Term of Clause" shall survive the termination of this Contract.

Any ambiguity in this Contract clause shall be resolved to permit Covered Entity to comply with he Rules implemented under HIPAA

H.9 CMS INFORMATION SECURITY (APR 2013)

All CMS information shall be protected from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction, whether accidental or intentional, in order to maintain the security, confidentiality, integrity, and availability of such information. Therefore, if this contract requires the Contractor to provide services (both commercial and non-commercial) for Federal Information/Data, to include any of the following requirements:

- Process any Information/Data; or
- Store any Information/Data (includes “Cloud” computing services); or
- Facilitate the transport of Information/Data; or
- Host/maintain Information/Data (including software and/or infrastructure developer/maintainers); or
- Have access to, or use of, Personally Identifiable Information (PII), including instances of remote access to, or physical removal of, such information beyond agency premises or control, the Contractor shall become and remain compliant with the requirements set forth at the CMS Information Security website at

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Information-Security-Contract-Clause-Provision.html. The requirements cover **all** CMS contracts and associated deliverables, which are required on a "per Contractor" basis.

The Contractor shall ensure that the following Federal information security standards are met for all of its CMS contracts:

- **Federal Information Security Management Act (FISMA)** – FISMA information can be found at http://csrc.nist.gov/groups/SMA/fisma/index.html. FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source; and,
- **Federal Risk and Authorization Management Program (FedRAMP)** – FedRAMP information can be found at http://www.gsa.gov/portal/category/102371. The FedRAMP is a Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

The Contractor shall include in all awarded subcontracts the FISMA/FedRAMP compliance requirements set forth at the CMS Information Security website at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Information-Security-Contract-Clause-Provision.html.

H.10 OPEN GOVERNMENT PROACTIVE PRE-DISCLOSURE NOTIFICATION (AUG 2013)

In order to reduce the administrative burden of responding to Freedom of Information Act (FOIA) requests for high visibility/high public interest contracts throughout contract administration, the Contractor shall submit its review of the awarded contract (and contract modifications, if requested) for FOIA disclosure exemptions within thirty (30) calendar days of contract award. The review will substantiate "…Trade secrets and commercial or financial information obtained from a person and privileged or confidential…" information, in accordance with 5 U.S.C. §552 FOIA, Exemption (b)(4), which could reasonably be expected to cause substantial competitive harm.

Submissions: The Contractor shall submit one (1) Compact Disc (CD) or Digital Video Disc (DVD) with all 5 U.S.C. §552 FOIA, Exemption (b)(4), "…Trade Secrets, Commercial or Financial Information Which is Privileged or Confidential…," otherwise known as public release/non-Confidential Business Information (non-CBI), with the information identified as follows:

a. **CBI Highlighted Copy of Contract**: One copy of the contract with all CBI highlighted for CMS FOIA review.

b. **Contractor Proposed Redacted Public Release Copy of Contract**: An additional copy of the contract will be provided for public release with all the identified information redacted. Redactions shall be made using "black" boxes, which cannot be removed or uncovered by a reader.

c. **Pre-Disclosure Concerns - Comments/Rationale for Non-Disclosure of Trade Secrets, Commercial or Financial Information Which is Privileged or Confidential**: The Contractor shall provide, in a separate file, rationale for why disclosure of "…Trade Secrets, Commercial or

Financial Information Which is Privileged or Confidential…" would cause the Contractor organization substantial competitive harm if disclosed to other entities. Rationale shall be provided for each individual recommended redaction. Generalized conclusions of competitive harm are not a sufficient basis for the CMS FOIA office to invoke the exemption and thereby protect the Contractor's interest.

All CD/DVDs shall be mailed to the CMS FOIA Officer (address below) within thirty (30) calendar days of contract award and within thirty (30) calendar days of a CMS request, i.e. existing or modified contracts. All CD/DVD files shall be submitted as Portable Document Format (.pdf) files.

CD/DVD and File Naming Conventions: The Contractor shall name the CD/DVD with the Contract Number and utilize the following CD/DVD file naming conventions:

HHSM-500-2013-xxxxxx – Highlighted
HHSM-500-2013-xxxxxx – Redacted
HHSM-500-2013-xxxxxx – Pre-Disclosure Concerns

CD/DVD shall be mailed to the CMS FOIA Officer at:

Centers for Medicare & Medicaid Services
Freedom of Information Act Office
ATTN: CMS FOIA Officer
Mailstop: N2-20-16
7500 Security Boulevard
Baltimore, MD 21244-1850

Copy– Correspondence Only (No CD/DVD):

Contracting Officer

Contracting Officer's Representative (COR)

It should be noted that the CMS FOIA Office makes the final determination as to what information is released to the public, after considering any feedback from OAGM and/or the Contractor.

H.11 SECTION 508, ACCESSIBILITY OF ELECTRONIC AND INFORMATION TECHNOLOGY (EIT)

A. This contract is subject to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by the Workforce Investment Act of 1998 (P.L. 105-220). Specifically, subsection 508(a)(1) requires that when the Federal Government procures Electronic and Information Technology (EIT), the EIT must allow all Federal employees and individuals of the public with disabilities comparable access to and use of information and data that is provided to Federal employees and individuals of the public without disabilities.

B. The EIT accessibility standards at 36 CFR Part 1194 were developed by the Architectural and Transportation Barriers Compliance Board ("Access Board") and apply to contracts and task/delivery orders, awarded under indefinite quantity contracts on or after June 25, 2001.

C. Each Electronic and Information Technology (EIT) product or service furnished under this contract shall comply with the Electronic and Information Technology Accessibility Standards (36 CRF 1194), as specified in the contract, as a minimum. If the Contracting Officer determines any furnished product or service is not in compliance with the contract, the Contracting Officer will promptly inform the Contractor in writing. The Contractor shall, without charge to the Government, repair or replace

the non-compliant products or services within the period of time to be specified by the Government in writing. If such repair or replacement is not completed within the time specified, the Government shall have the following recourses:

1. Cancellation of the contract, delivery or task order, purchase order, or line item without termination liabilities; or

2. In the case of custom EIT being developed by a Contractor for the Government, the Government shall have the right to have any necessary changes made or repairs performed, by itself, or by another firm for the non-compliant EIT, with the Contractor liable for reimbursement to the Government for any expenses incurred thereby.

D. The contractor must ensure that all EIT products that are less tan fully compliant with the accessibility standards are provided pursuant to extensive market research and are the most current compliant products or services available to satisfy this contract's requirements.

E. For every EIT product or service accepted under this contract by the Government that does not comply with 36 CRF 1194, the contractor shall, at the discretion of the Government, make every effort to replace or upgrade it with a compliant equivalent product or service, if commercially available and cost neutral, on either the planned refresh cycle of the product or service, or on the contract renewal/effective option date, whichever shall occur first.

F. The contractor shall comply with the Rehabilitation Action, Section 508, Accessibility Standards as referenced below.

508 Standards: http://www.access-board.gov/sec508/standards.htm

Guide to Standards: http://www.access-board.gov/sec508/guide/index.htm

508 guide: http://cmsnet.cms.hhs.gov/hpages/cmm/dmsd/508Ref_Guide.doc

H.12 Notice of the potential for Termination for Convenience in accordance with 52.249-2 -- Termination for Convenience of the Government (Fixed-Price).

Each offeror should be aware that this requirement is entirely new, however the model in which this requirement is meant to test has been underway since December 9, 2011 with the award of the original 26 HEN contracts.

CMS will receive in August of 2015 the final data required to submit to OACT for a final determination that may result in an expansion, a continuation or a termination of activities related to the entire program.

CMS must in an effort to provide complete transparency, advise all potential offerors that in the event OACT's determination is to terminate this program, all HEN 2.0 contracts must be terminated for convenience in accordance with FAR 52.249-2 Termination for Convenience of the Government (Fixed Price).

H.13 DUPLICATION OF EFFORT

The government must make it clear that duplication of effort shall not be allowed as it relates to quality improvement efforts such as the HENs/QIO/QIN contracts, and TCPI grants.

The contractor hereby certifies that costs for work to be performed under this contract and any subcontract hereunder are not duplicative of any costs charged against any other Government contract, subcontract, or other Government source. The contractor agrees to advise the Contracting Officer, in writing, of any other Government contract or subcontract it has performed or is performing which involves work directly related to the purpose of this contract. The contractor also certifies and agrees that any and

all work performed under this contract shall be directly and exclusively for the use and benefit of the Government, and not incidental to any other work, pursuit, research, or purpose of the contractor, whose responsibility it will be to account for it accordingly.